

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

07/31/2013

SUBJECT:

Cisco WAAS Central Manager Remote Code Execution Vulnerability

OVERVIEW:

Cisco Wide Area Application Services (WAAS) when configured as Central Manager (CM), contains a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on the affected system.

SYSTEMS AFFECTED:

The following products running a vulnerable version of Cisco WAAS Software and configured as Central Manager (CM) are affected by this vulnerability:

- Cisco WAAS Appliances
- Cisco Virtual WAAS (vWAAS)
- Cisco WAAS Modules

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

DESCRIPTION:

A vulnerability in the web service framework code of Cisco WAAS, when configured as Central Manager (CM) could allow an unauthenticated, remote attacker to execute arbitrary code on the affected system.

The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted POST request to the affected system. An exploit could allow the attacker to execute arbitrary code on the affected system. Due to the privileged function of

the WAAS CM in the Cisco WAAS network, exploitation of this vulnerability could allow the attacker to gain administrative access to all the devices that have been associated to the vulnerable WAAS CM.

RECOMMENDATIONS:

The following actions should be taken:

- Update the WAAS devices on vulnerable systems using the instructions provided by Cisco <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130731-waascm>

REFERENCES:

Cisco:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130731-waascm>